IMPACT BOARDS
EMERGING MARKETS

DIRECTORS VIEW

Gretta Antonescu

Non-Executive Director, Member of The Board of Advisors – qodeo

BoD Audit & Risk Committee priorities 2024: Navigating Cybersecurity Regulations on monitoring and reporting

The ever-shifting business landscape and stakeholder expectations are driving a constant update to regulations and reporting standards. This puts immense pressure on Audit Committees (ACs) to stay abreast of these changes and adapt their mandates accordingly.

With cyber threats escalating, cybersecurity has become a top priority for regulators. Consequently, the responsibility for oversight has fallen squarely on the shoulders of boards' Audit and Risk Committees.

Before we delve into the new regulations, let's establish a clear understanding of cyber events. The National Institute of Standards and Technology (NIST) defines a cyber event as any occurrence that:

- Threatens the confidentiality, integrity, or availability of information systems or data. This means information could be stolen, corrupted, made inaccessible, or used in unauthorized ways.
- Violates established security policies or procedures. This includes any actions that bypass security measures or disregard security protocols.

In the US, the SEC and Public Company Accounting Oversight Board (PCAOB) have ambitious agendas for 2024 and beyond, with new rules focusing on critical areas like: cybersecurity, executive compensation, and financial restatements. These regulations will likely necessitate significant investments in compliance systems, processes, and training for both top management and boards of directors.

In the European Union, the EU's Network and Information Systems Security (NIS2) Directive marks a significant step towards strengthening Europe's cyber defenses by mandating four key actions for organizations: risk management, accountability, incident reporting, and business continuity. Beyond the core requirements, NIS2 mandates essential and important entities to implement specific security measures to combat potential cyber threats. These 10 measures focus on: Risk Assessment & Policies; Security Measure Effectiveness; Cryptography & Encryption; Incident Response Planning; Secure Development & Procurement; Cybersecurity Awareness & Training; Data Access Control; Business Continuity Management; Advanced Authentication; Supply Chain Security. Compliance is mandatory, requiring organizations to:

- Report significant cybersecurity incidents within 24 hours (less significant within 72 hours).
- Implement harmonized administrative fines and ensure compliance readiness by October 2024.
- Foster Corporate Accountability by mandating CEO, BoD oversight, approval, and training on cybersecurity measures.

Uncertain Path: The Impact of NIS2 on Emerging Markets

The new EU Cybersecurity regulations (NIS2) hold both promise and peril for emerging markets. The overall impact will hinge on several factors:

- **Implementation Specificity:** How individual countries translate NIS2 into national regulations will significantly influence its effect.
- **Government Support:** The level of government aid, financial or educational, will influence a country's ability to adapt to the new standards.
- **Company Capabilities:** Existing cybersecurity infrastructure and resources within emerging market companies will determine their ability to comply.
- **Supply Chain Risks:** The NIS2 directive extends to supply chains. Companies in emerging markets might struggle to ensure their entire supply chain (including foreign partners) complies with the regulation.

While challenges exist, NIS2 could also unlock positive outcomes for emerging markets:

- **Improved Security Posture:** The regulations could act as a catalyst for improved cybersecurity practices across emerging economies.
- **Level Playing Field:** Adherence to NIS2 could create a more balanced market for emerging companies competing with EU businesses.
- **Increased Awareness:** The regulations may raise the overall cybersecurity awareness within emerging markets, leading to a more secure digital environment.

The Call to Action: Proactive Engagement is Essential

Whilst the overall impact of NIS2 on emerging markets will depend on several factors, at company level, by proactively engaging with management in preparation for upcoming disclosures, boards can ensure they are well-informed, compliant, and prepared to effectively communicate with stakeholders.

For **boards seeking a proactive stance on cybersecurity**, the **Audit and Risk Committee** can take the initiative by:

- Conducting a comprehensive cybersecurity self-assessment to evaluate the organization's cybersecurity posture across people, processes, and technology.
- **Implementing a robust cybersecurity checklist** to identify key controls and best practices, and be used for ongoing monitoring and improvement.
- **Scheduling regular reviews and validations of the self-assessment and checklist** to ensure ongoing effectiveness and adaptation to evolving threats.

By taking these proactive steps, the Audit and Risk Committee can empower the board to make informed decisions and ensure the organization is well-prepared to address evolving cyber threats.